Arttu Virta

KÄYTTÄYTYMISBIOMETRIIKKA TIETOTURVALLISUUDEN TYÖKALUNA.

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Virta, Arttu
Käyttäytymisbiometriikka tietoturvallisuuden työkaluna
Jyväskylä: Jyväskylän yliopisto, 2024, s29
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Siitonen, Valtteri

Tässä kandidaatintutkielmassa tarkastellaan käyttäytymisbiometriikan soveltuvuutta tietoturvallisuuden parantamiseen. Tutkielma keskittyy erityisesti hiiri-, kosketusnäyttö- ja näppäilydynamiikan käyttöön ja vertaa näitä fyysisen biometriikan menetelmiin, kuten sormenjälkiin. Lisäksi tutkielma käsittelee käyttäytymisbiometriikasta kerättävän tiedon keräystä ja käsittelyä. Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielma ehdottaa käyttäytymisbiometriikan hyödyntämistä tietoturvallisuuden parantamiseen sekä kehottaa lisäämään aiheen tutkimusta tulevaisuudessa. Tutkielmassa korostetaan myös käyttäytymisbiometriikan haasteita, jotka liittyvät yksityisyydensuojaan ja datan keräämisen ongelmiin, joista menetelmä on voimakkaasti riippuvainen.

Asiasanat: Tunnistautuminen, biometriikka, tietoturva, käyttäytymisbiometriikka

ABSTRACT

Virta, Arttu
Behavioral Biometrics as a Tool for Information Security
Jyväskylä: University of Jyväskylä, 2024, 29p.
Information Systems, Bachelor's Thesis
Supervisor(s): Siitonen, Valtteri

This bachelor's thesis examines the applicability of behavioral biometrics for enhancing information security. The thesis particularly focuses on the use of mouse dynamics, touchscreen interactions, and keystroke dynamics, and compares these to physical biometrics such as fingerprints. Furthermore, the thesis addresses the collection and processing of data derived from behavioral biometrics. The thesis is conducted as a literature review. It suggests utilizing behavioral biometrics to improve information security and advocates for increased research into the subject in the future. The thesis also highlights the challenges associated with behavioral biometrics, particularly concerning privacy protection and the problems related to data collection, on which the method heavily depends.

Keywords: Authentication, biometrics, information security, behavioral biometrics

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Biometrinen tunnistautuminen on kehittynyt merkittäväksi tekniikaksi henkilöllisyyden varmentamisessa nykymaailmassa, jossa yhä kasvavassa määrin korostuu tarve luotettavalle käyttäjän autentikoinnille. Tarve johtuu digitaalisten palveluiden yleistymisestä ja niiden mukana kasvavista turvallisuushuolista. (Jain ym., 2006)

Perinteisesti henkilöiden tunnistamisessa on laajalti käytetty yksinomaiseen hallintaan perustuvia tunnisteita, kuten passia tai henkilökorttia. Tietokonejärjestelmissä ja sovelluksissa tunnistautumiseen käytetään yleisesti tietoon perustuvia menetelmiä, kuten salasanoja ja PIN-koodeja. Sekä tunniste- että tietoon perustuvilla mekanismeilla on omat vahvuutensa ja rajoituksensa. (Jain ym., 2016)

Biometrinen tunnistautuminen on yleistynyt erityisesti 2000-luvulla paikkaamaan perinteisten menetelmien heikkouksia ja on toiminut ensisijaisena tunnistautumismenetelmänä esimerkiksi puhelimissa, tietokoneissa ja muissa kuluttajaelektroniikan tuotteissa. Biometrisen tunnistautumisen suosiolle on monia syitä, joista He ja Wang (2015) tunnistavat seuraavat tekijät merkittävimmiksi eduiksi:

1. Biometrisiä tietoja on vaikea hukata tai unohtaa
2. Biometrisiä tietoja on vaikea kopioida tai jakaa
3. Biometriikan väärentäminen tai levittäminen on vaikeaa
4. Biometrisiä tietoja on vaikea arvata
5. Biometristen tietojen murtaminen on vaikeampaa

Digitaalisten palveluiden käytön lisääntyessä ja tietoturvauhkien kehittyessä on kehitettävä uusia tietoturvan menetelmien käyttäjien valvontaan ja varmentamiseen. Perinteisesti biometrisessä tunnistautumisessa hyödynnetään käyttäjien fyysisiä piirteitä osana tunnistautumisprosessia (Jain ym., 2016). Uudempi biometrisen tunnistautumisen muoto, käyttäytymisbiometriikka, puolestaan hyödyntää käyttäjien käytöksellisiä piirteitä. Chyzhveska ym. (2022) tunnistavat

käyttäytymisbiometriikan potentiaalin tietoturvallisuuden työkaluna, sillä käyttäytymisbiometriikka paikkaa useita sekä fyysisen biometriikan että perinteisten menetelmien heikkouksia. Lisäksi käyttäytymisbiometriikan ainutlaatuiset ominaisuudet mahdollistavat uudenlaisten tietoturvatyökalujen kehittämisen, jotka eivät ole olleet toteutettavissa aiemmilla teknologioilla.

Tässä tutkielmassa termiä "biometriikka" suositaan termin "biometria" sijaan. MOT-sanakirja (2024) määrittää biometrian biologisen materiaalin keräämisen ja analysoinnin prosessiksi. Toisin sanoen, se keskittyy elävien organismien, erityisesti ihmisen, fyysisten ja fysiologisten ominaisuuksien kvantitatiiviseen mittaukseen. Biometriikka puolestaan määritellään MOT-sanakirjan (2024) mukaan laajemmin tunnistautumisen ja identifioinnin prosessiksi, joka perustuu yksilön ainutlaatuisiin fyysisiin tai käyttäytymiseen liittyviin piirteisiin. Tämä määritelmä ei rajoitu pelkästään biologisen datan keruuseen, vaan kattaa myös laajemman spektrin attribuutteja, mukaan lukien käyttäytymismallit ja jopa abstraktimmat piirteet, jotka ovat identifioitavissa ja mitattavissa teknologisen edistyksen myötä.

Perinteisesti biometrisessä tunnistautumisessa on käytetty fyysisiä piirteitä, joka on yleistänyt termin ”biometria” käytön tunnistautumisen prosesseissa, mutta termi ”biometriikka” on yleistynyt käytöksellisen tunnistautumisen edistyessä.

Tämän tutkielman tavoitteena on tutkia ja esitellä käyttäytymisbiometriikan menetelmiä, niiden käyttöä sekä varteenotettavuutta tietoturvallisuuden työkaluna. Tutkielmassa vertaillaan fyysiseen biometriikkaan perustuvia varmentamismenetelmiä käyttäytymisbiometrisiin menetelmiin. Vertailun perusteella arvioidaan näiden menetelmien varteenotettavuutta ja tehokkuutta tietoturvan näkökulmasta. Tarkoituksena on esitellä käyttäytymisbiometriikan menetelmiä tietoturvallisuudessa ja tarkastella niiden tehokkuutta.

Tutkielman tutkimuskysymykset ovat seuraavat:

- Miten käyttäytymisbiometriikkaa voidaan hyödyntää tietoturvallisuudessa?
- Kuinka varteenotettava tietoturvallisuuden työkalu käyttäytymisbiometriikka on?

Tutkielma on toteutettu kirjallisuuskatsauksena. Lähdeaineisto on haettu pääsääntöisesti Web of Science- ja Google Scholar -tietokannoista. Hakutermeinä on käytetty muun muassa biometrics, behavioral biometrics, security, authentication ja dynamics. Lähdeaineistoksi valittiin mahdollisimman tuoreita artikkeleita siten, että lähes kaikki artikkelit on julkaistu vuoden 2010 jälkeen. Poikkeukset koskevat artikkeleita, jotka käsittelevät aiheen historiaa tai sisältävät olennaisia määritelmiä. Tuoreuden lisäksi lähteiksi pyrittiin valitsemaan artikkeleita, joilla oli mahdollisimman paljon viittauksia. Aiheen ajankohtaisuuden vuoksi

lähdeaineistoon sisällytettiin myös uusia tutkimuksia, joilla ei vielä ole paljon viittauksia tuoreutensa vuoksi. Tutkielmassa hyödynnettiin lisäksi aihetta sivuavia tutkimuksia vertailun vuoksi.

Tutkielman sisältö jatkuu ensimmäisessä sisältöluvussa tunnistautumisen menetelmien sekä tietoturvan määrittelyllä. Lisäksi käsitellään tarkemmin biometristä tunnistautumista ja sen piirteitä. Toisessa sisältöluvussa käsitellään käyttäytymisbiometriikan menetelmiä ja verrataan niitä fyysisen biometriikan menetelmiin. Lisäksi tutkitaan käyttäytymisbiometriikan tehokkuutta, siihen liittyviä haasteita, hyötyjä sekä tulevaisuuden näkymää. Tutkielman päättää yhteenveto, jossa kootaan tutkielman sisältö ja siinä käsitellyt aiheet.

2 TUNNISTAUTUMINEN TIETOTURVALLISUUDESSA

Tässä luvussa käsitellään tietoturvaa ja tunnistautumista sekä määritellään tutkielman keskeisiä käsitteitä.

2.1 Tietoturva

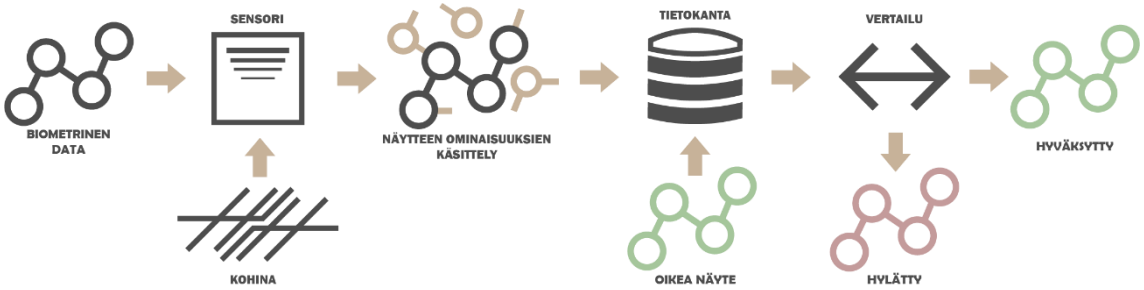
Tietoturva on keskeinen tekijä informaation ja tietojärjestelmien suojaamisessa nykyaikaisissa organisaatioissa ja kattaa laajan kirjon ominaisuuksia ja erilaisia määritelmiä. IATE (2024) määrittelee tietoturvan kolmen osa-alueen, luotettavuuden (confidentiality), eheyden (integrity) ja saatavuuden (availability) turvaamisen prosessiksi, joka tunnetaan myös CIA-mallina. Suomen tietosuojavaltuutetun toimisto (2024) määrittää tietoturvan tietosuojan toteutuksen keinoksi, jossa tietoturvan keinoilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys ja käyttäjien oikeuksien toteutuminen. Vaikkakin CIA-malli on kokenut kritiikkiä tietoturvan määritelmänä (Lundgren & Möller, 2017), on se toistaiseksi yleisimmin käytetty määritelmä tietoturvalle.

Tietoturvan merkitys kasvaa jatkuvasti, ja se on elintärkeä elementti sekä yrityksille että hallinnoille (von Solms, 2001), joista valtaosa on ottanut käyttöön erilaisia tietoturvakäytänteitä (Alotabi ym., 2016). Tietoturvan rooli on perinteisesti ollut yritysten ja hallintojen tukitoimintona, mutta digitalisaation edetessä siitä on muodostumassa keskeinen edellytys toiminnan jatkuvuudelle ja menestykselle.

Tietoturvassa tunnistautumista käytetään yksityisyyden suojaamiseen tähtäävänä prosessina (Barbosa ym., 2008), jonka tarkoituksena on varmistaa oikeudenmukainen pääsy asianmukaisiin resursseihin.

2.2 Biometrinen tunnistautuminen yleisesti

Biometrisellä tunnistautumisella tarkoitetaan tunnistautumisen menetelmää, jossa yksilön varmennushetkellä saatua biometristä tietoa verrataan laitteeseen tallennettuun biometriseen malliin (eli yksi-yhteen vastaavuuden tarkastusprosessi). Biometrinen tieto puolestaan koostuu henkilötiedoista, jotka syntyvät tietyn teknisen käsittelyn seurauksena ja liittyvät henkilön fyysisiin, fysiologisiin tai käyttäytymiseen liittyviin ominaisuuksiin, kuten kasvonpiirteisiin tai sormen jälkiin, jotka mahdollistavat kyseisen henkilön yksilöllisen tunnistamisen. (IATE, 2024) Biometrisen tunnistautumisen määritelmä voi vaihdella eri tieteenaloilla, mutta informaatioteknologiassa sillä tarkoitetaan tyypillisesti henkilön identiteetin varmentamista biologisella informaatiolla. (Bhattacharyya ym., 2009)



KUVIO 1 Biometrisen tunnistautumisen prosessi. (Mukaillen Jain ym., 2016 ja IATE, 2024)

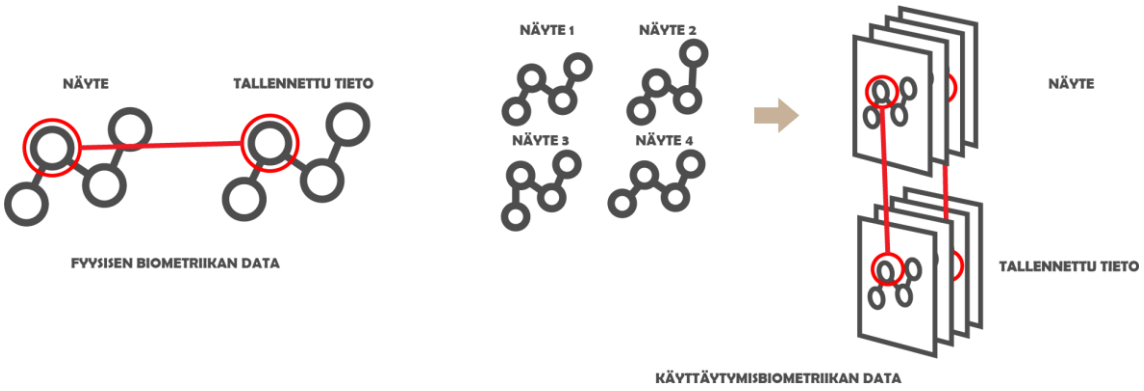
2.2.1 Fyysinen biometriikka (Physical biometrics)

Fyysisellä biometriikalla tarkoitetaan biometrisen tunnistautumisen menetelmiä, jotka tarjoavat tapoja yksilöidä ja tunnistaa käyttäjiä käyttäen heidän fysiologisia ominaisuuksiaan. Biometrics Institute (2024) määrittää fyysisen biometriikan attribuuteiksi ihmisen fyysiset, rakenteelliset ja suhteellisen muuttumattomat ominaisuudet, kuten sormenjäljet, silmän rakenteen, kasvojen ääriviivat tai laskimoiden geometrian. Jotkin attribuutit voivat olla myös mikroskooppisia luonteeltaan, esimerkiksi DNA tai ihmisen haju. Bhattacharyya ym. (2009) lisäävät, että fyysisen biometriikan kriteerinä on tarpeellinen erilaisuus (katso kuvio 3), jotta ominaisuus pystytään erottamaan yksilöiden välillä.

Fyysistä biometriikkaa on sovellettu laajasti jo kuluttajaelektroniikassa esimerkiksi sormenjälkitunnistamisen tai kasvojen skannauksen muodossa. Fyysistä biometriikkaa on pidetty perinteisesti käyttäytymisbiometriikkaa luotettavampana, ja tämän takia kokenut laajempaa implementaatiota (Bailey ym., 2014)

2.2.2 Käyttäytymisbiometriikka (Behavioral biometrics)

Käyttäytymisbiometriikka on biometrisen tunnistautumisen menetelmä, joka mittaa miten käyttäjät suorittavat tiettyjä toimintoja. Tämä biometrisen tunnistautumisen alue erottuu fyysisestä biometriikasta siinä, että se perustuu oppimiimme ja toistettaviin toimintoihin, kuten kirjoittamiseen, puheeseen tai kävelytyyliin, eikä pysyviin fyysisiin ominaisuuksiin. Käyttäytymisbiometriikassa kerätään dynaamisia näytteitä ja tietoja kohteesta, joka vaikeuttaa tietojen kaappaamista ja väärinkäyttöä. Fyysisen biometriikan attribuuteista kerätään tyypillisesti kertaluontoiset näytteet, esimerkiksi sormenjälki, mikä voi altistaa sen väärinkäytölle. (Ballard ym., 2007) Käyttäytymisbiometriikan mittaamisessa hyödynnetään usein myös ajallisia jaksoja ja mittauksia. Näytteitä otetaan useita pitkällä ajanjaksolla ja yksittäisen näytteiden vertaamisen lisäksi verrataan myös niiden ajallista kehitystä. Näytteiden määrällä voidaan määritellä käyttäjäprofiilin monipuolisuus ja tarkkuus, joka puolestaan mahdollistaa entistä varmemman tunnistautumisen menetelmän.



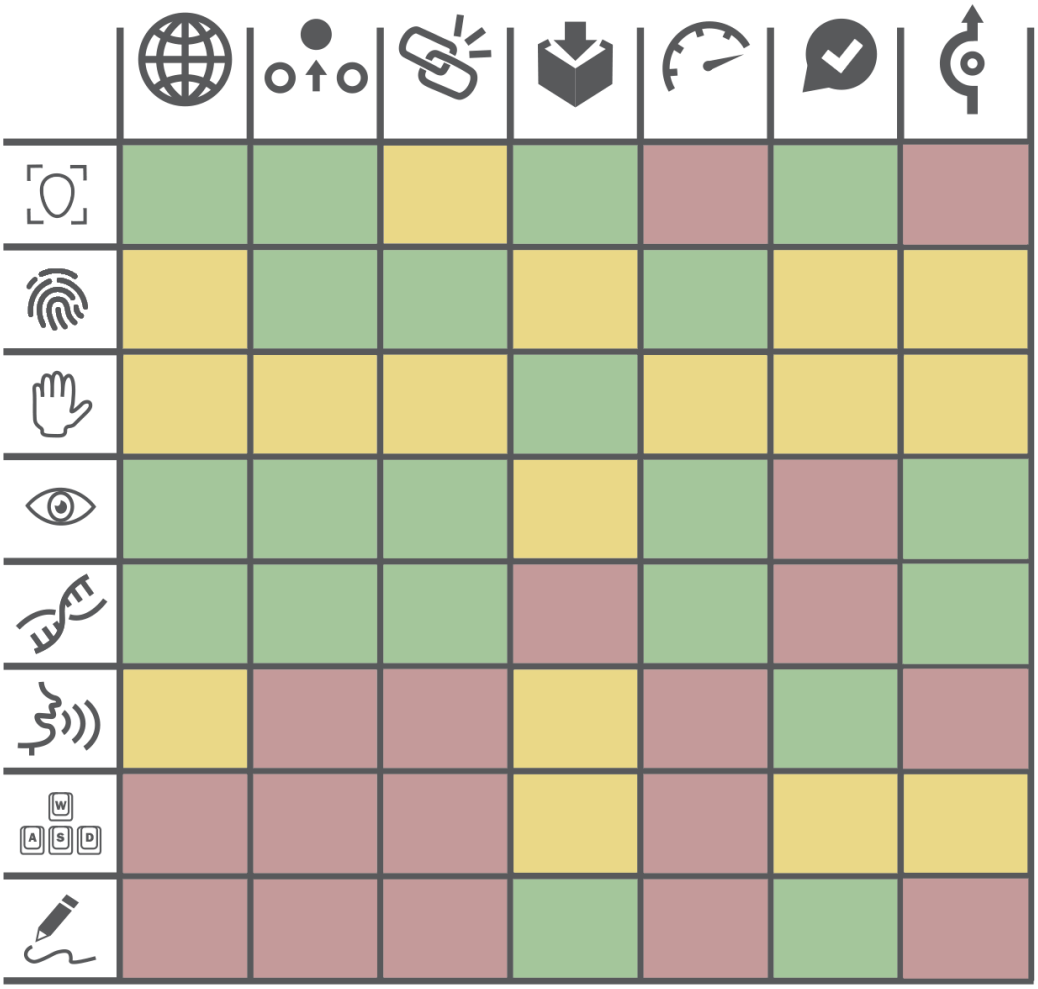
KUVIO 2 Datan keräämisen ja vertailun ero fyysisellä biometriikalla ja käyttäytymisbiometriikalla.

Osa biometrisen tunnistautumisen menetelmistä, kuten ääni, sisältää piirteitä sekä käyttäytymisbiometriikasta että fyysisestä biometriikasta, jolloin sen kategorisointi perustuu mitattaviin ominaisuuksiin. (Bhattacharyya ym., 2009)

2.2.3 Biometriikan piirteet

O'Gorman (2003) luokitteli biometriikan menetelmät alun perin vakauden perusteella, joko vakaiksi tai epävakaiksi menetelmiksi. Vakaat biometriset attribuutit, kuten sormenjäljet, kasvot, iiris ja käsi, ovat ajan myötä melko muuttumattomia ja niiden ominaisuudet vakiintuvat yleensä aikuisuuteen mennessä. Vastaavasti muuttuvat biometriset attribuutit, kuten puhe tai käsiala, sisältävät muuttujia, jotka tekevät niiden esiintymisestä dynaamista. Tämän erottelun tärkeys korostuu etenkin tietoturvallisuudessa, jossa vakaiden biometristen signaalien käyttö tarjoaa lähtökohtaisesti luotettavamman varmentamisprosessin.

Biometriikan käytön yleistyessä ja sen teknologioiden kehittyessä, Jain ym. (2006) ja myöhemmin Odelu ym. (2015) ovat laajentaneet näkemystä biometriikan ominaisuuksista kuvaamalla erilaisia haavoittuvuuksia ja potentiaalisia riskejä, joita näihin menetelmiin liittyy. Heidän tutkimuksensa korostavat, kuinka biometriset menetelmät voivat olla alttiita teknisille ja sosiaalisille hyökkäyksille, jotka voivat vaarantaa henkilötietojen turvallisuuden.



= Kasvot = Sormenjälki = Käsigeometria = Iiris
= DNA = Ääni = Näppäily = Allekirjoitus

= Yleisyys (Universality). Kuvaa sitä, löytyykö tunnistettava piirre kaikilta ihmisiltä

=Erilaisuus (Distinctiveness). Viittaa siiheen, onko mitattava ominaisuus uniikki kaikilla ihmisillä.

= Pysyvyys (Permanence). Kuvaa, kuinka muuttumaton mitattava ominaisuus on.

= Kerättävyys (Collectable). Ilmaisee, kuinka hyvin tunnusmerkkejä voidaan kerätä ja kvantifioida.

= Suorityskyky (Performance). Kuvaa menetelmän biometrisen järjestelmän nopeutta ja tarkkuutta.

= Hyväksyttävyys (Acceptability). Kuvaa käyttäjien halukkuutta menetelmän hyväksymiseen ja käyttöön.

= Kiertäminen (Circumvention). Kuvaa biometrisen menetelmän ja sen järjestelmän haavoittuvuutta ja sitä, kuinka helppoa on huijata tai ohittaa sen käyttö.

KUVIO 3 Biometristen menetelmien suoriutuminen. (Mukaillen Jain ym., 2006 ja Odelu ym., 2015)

2.3 Perinteiset tunnistautumisen menetelmät

Perinteiset tunnistautumismenetelmät, kuten salasanat, luokitellaan tyypillisesti ”tietopohjaisiksi” (knowledge based) tunnistautumisen menetelmiksi. Tämän tapaisissa tunnistautumisen menetelmissä tunnistautuminen nojautuu ennalta määritettyyn tietoon, kuten merkki-, numero- tai symbolijonoon. Biometrisen tunnistautumisen menetelmät puolestaan luokitellaan ”ID-pohjaisiksi”, jossa tunnistautumiseen käytettävät ominaisuudet ovat luonnostaan uniikkeja eri käyttäjillä. (O’Gorman, 2013)

Tietopohjaisia tunnistautumismenetelmiä pidetään tarkkoina ja toimivina, mutta asettavat haasteita erityisesti tunnistautumiskohteiden lisääntyessä. Tietopohjaiset menetelmät toimivat yleisimpänä tunnistautumismenetelmänä ja käyttäjät tyypillisesti toistavat, esimerkiksi salasanoja tai PIN-koodeja, useiden kohteiden välillä. Useiden salasanojen muistaminen luo taakkaa käyttäjille ja salasanojen mahdollinen urkkiminen, vuotaminen tai murtaminen ovat riski. (Lien & Vhaduri, 2023).

Vahva tunnistautuminen on suosiota nostanut tunnistautumisen menetelmä, joka yhdistää vähintään kaksi teknisesti erilaista tunnistautumisen menetelmää (Kyberturvallisuuskeskus, 2024). Menetelmä pyrkii paikkamaan tunnistautumisen menetelmien heikkouksia yhdistelemällä esimerkiksi salasanoja ja sormenjälkitunnistusta. Menetelmää hyödynnetään erityisesti kriittisemmissä tietoturvakohteissa.

3 KÄYTTÄYTYMISBIOMETRIIKKA KÄYTÄNNÖSSÄ

Tässä luvussa esitellään yleisimpiä käytössä olevia fyysisen biometriikan sekä käyttäytymisbiometriikan menetelmiä. Lisäksi käsitellään niiden esiintymistä käytännössä ja yleistä tehokkuutta. Luvun lopussa käsitellään käyttäytymisbiometriikan keskeisiä haasteita ja pohditaan sen tulevaisuutta.

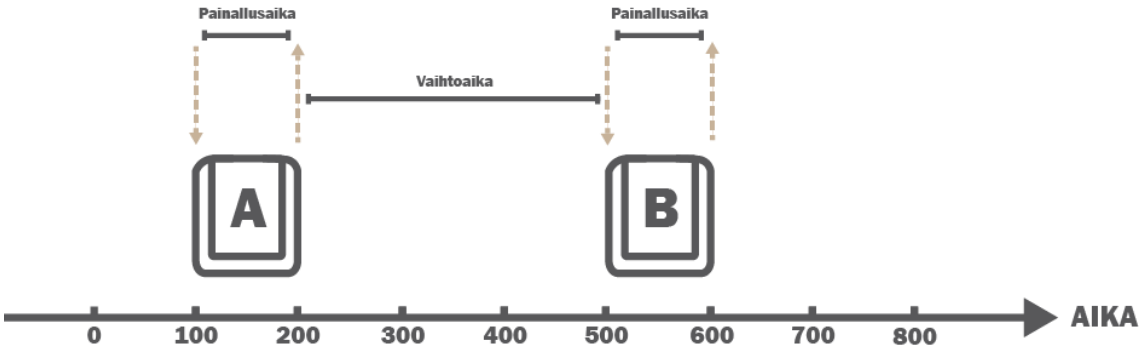
3.1 Biometrisen tunnistautumisen menetelmiä

Sormenjälkitunnistus on yksi yleisimmistä fyysisen biometriikan menetelmistä ja se hyödyntää käyttäjän sormenjälkien ainutlaatuisia kuvioita käyttäjän henkilöllisyyden varmistamiseksi tai tunnistamiseksi. Sormenjälkitunnistus hyödyntää kuviossa yksi esitettyä prosessointia varmistaakseen käyttäjän henkilöllisyyden vertaamalla annettua sormenjälkinäytettä tietokannassa olevaan varmennettuun tietoon. (Yang ym., 2019) Kasvojentunnistus on myös laajassa käytössä oleva fyysisen biometriikan menetelmä. Kasvojentunnistus hyödyntää käyttäjien kasvojen uniikkeja piirteitä samankaltaisesti kuin sormenjälkitunnistus. Kasvojentunnistuksessa voidaan käyttää datapisteinä kaksiulotteisia piirteitä, kuten huulten, kulmakarvojen ja silmien kokoa sekä niiden suhteellisuutta toisiinsa. Lisäksi menetelmä voi hyödyntää kolmeulotteisia piirteitä tai kasvoista syntyviä lämpöjälkiä, mikä parantaa tunnistustarkkuutta ja luotettavuutta. (Albakri & Alghowinem, 2018)

3.1.1 Käyttäytymisbiometriikan menetelmiä

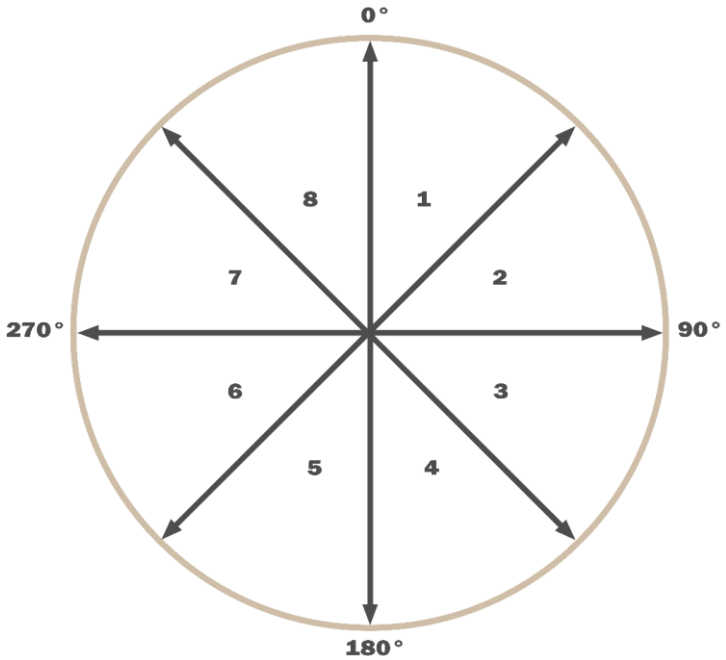
Näppäilydynamiikka on yksi käyttäytymisbiometriikan muodoista, joka perustuu käyttäjän näppäimistön käyttötavan mittaamiseen. Tämä menetelmä mahdollistaa henkilöllisyyden tunnistamisen tarkkailemalla, miten ja millä nopeudella käyttäjä painaa näppäimiä. Näppäilydynamiikan mittaus keskittyy moniin eri tekijöihin, kuten painallusten väliseen aikaan, painallusten kestoon ja niiden voimakkuuteen. Nämä mitatut ominaisuudet muodostavat käyttäjäkohtaisen

profiilin, joka voi sisältää yksityiskohtaisia tietoja siitä, miten yksilö käyttää näppäimistöä. (El-Kenawy ym., 2022) Näppäilydynamiikan keskeisin etu on siihen liittyvän datan keräämisen helppous ja datan toistettavuus luotettavasti. (Tewari & Verma, 2022)



KUVIO 4 Näppäilydynamiikan datan kerääminen. (Mukaillen Altwaijry, 2023).

Hiiridynamiikka on hyvin samankaltainen biometriikan muoto, jossa mittaamisen periaatteita sovelletaan käyttäjän käden liikkeisiin osana osoittimen liikuttamista. Esimerkiksi kuviossa viisi hiiren liikkeen suunnan määrittämiseksi lasketaan kulma liikkeen aloitus- ja lopetuskoordinaattien välillä. Tämän jälkeen määritetään liikkeen nopeus käyttämällä etäisyyskaavaa ja liikkeen aloitus- ja lopetusajankohtiin liittyviä aikaleimoja. (Bailey ym., 2014) Datan pohjalta voidaan käyttäjän hiirikäyttäytymisen pohjalta luoda yksilöity profiili.



KUVIO 5 Hiiridynamiikan datan kerääminen. (mukaillen Ahmed & Traore, 2007)

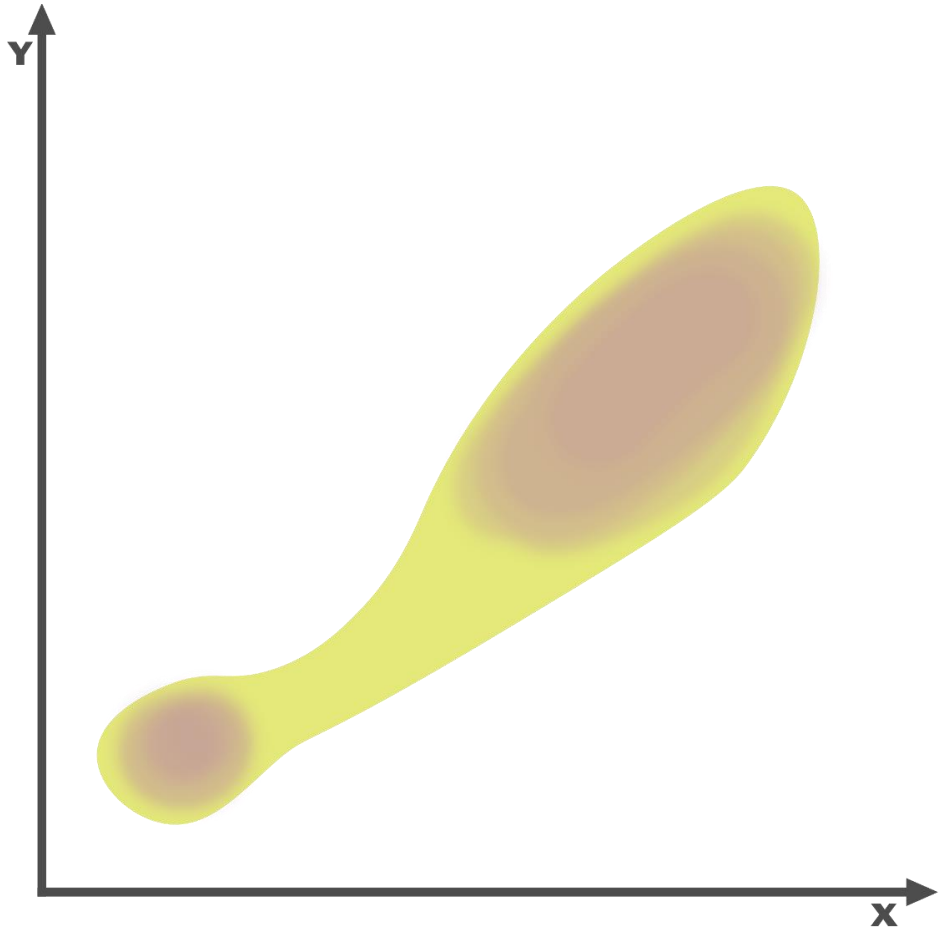
TypingDNA (2024) luonnehtii hiiri- ja näppäilydynamiikkaa sekä niiden yhdistelmää vahvaksi autentikoinnin metodiksi, jossa muodostetaan käyttäytymisperusteisia profiileja käyttäjästä.

Puheentunnistusta kuvaillaan usein menetelmänä, joka mahdollistaa käyttäjän ohjata elektronisia laitteita puheen avulla sen sijaan, että käytettäisiin perinteisiä syöttömenetelmiä, kuten näppäimistöä tai painikkeita. Puheentunnistusohjelmisto muuntaa käyttäjän puhumat sanat ja lauseet koneen ymmärtämään muotoon, mikä mahdollistaa laitteen helpon käytön puheen kautta. (Pahwa ym., 2020)

Puheen- ja äänentunnistus on jo pidempään tutkittu biometriikan menetelmä, mutta noussut vasta hiljattain varsinaiseen käyttöön biometriikassa. Puheen- ja äänentunnistuksen prosessit hyödyntävät kuviossa kolme kuvattua pidemmän aikavalin näytteenottoa, jonka prosessointi on haastavaa edeltäville teknologioille.

Nassif ym. (2016) kuvaa puhetta ihmisten välisen viestinnän perusmuotona ja tämän takia se on myös herättänyt huomattavaa kiinnostusta erityisesti koneoppimisen sekä tekoälyn prosesseissa. He kuvaavat tutkielmassaan useita erilaisia algoritmeja ja prosessointimalleja, mutta äänen ja puheen monimuotoisuus asettavat haasteita, jopa edistyneimmille algoritmeille. Prosessoinnin vaikeus voi selittää, miksi puheen- ja äänentunnistusta on sovellettu vain esimerkiksi saneluissa tai automaattisissa tekstityksissä ja tietoturvallinen soveltaminen on jäänyt vähäiseksi.

"Touchalytics", joka edustaa kosketusnäyttöön perustuvaa käyttäytymisbiometriikan muotoa, on kasvattanut suosiotaan kosketusnäyttölaitteiden yleistymisen myötä. Frank ym. (2013) määrittävät menetelmän jatkuvana tunnistautumisen menetelmänä, joka hyödyntää kosketusnäyttöä käyttäjän tunnistamiseen, perustuen erilaisiin käyttäytymispiirteisiin, kuten kosketuksen kestoon, paineeseen ja liikeratoihin.



Y = Näytöllä kuljettu matka pituussuunnassa. X = Näytöllä kuljettu matka leveyssuunnassa. Paksumpi viiva/ohuempi viiva = Kosketuksen hitaus/nopeus. Keltainen/punainen väri = Kosketuksessa käytetty vähemmän/enemmän voimaa.

KUVIO 6 Esimerkki kosketusdynamiikan datan keräämisestä.

Edellä mainittujen menetelmien lisäksi käyttäytymisbiometriikkaa pyritään laajentamaan ihmisen kehon liikehdinnän, katseen seurannan ja digitaalisen käyttäytymisen analysointiin, mutta kyseisiä menetelmiä ei ole vielä tutkittu tarpeeksi.

3.2 Käyttäytymisbiometriikan tehokkuus

Vertailuna fyysiseen biometriikkaan perustuva, sormenjälkiä hyödyntävä, tunnistautumisen menetelmä pystyy algoritmista riippuen saavuttamaan 0.022 % tasavirheasteen (EER) mikä vastaa yli 99,9 % tarkkuutta (Yang ym. 2019). Myös

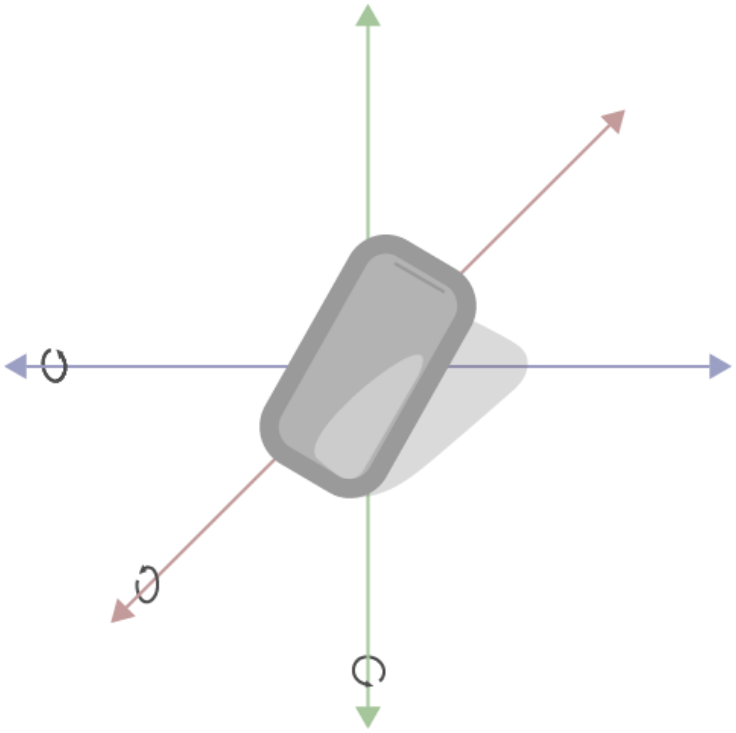
muut fyysisen biometriikan menetelmät saavuttavat tyypillisesti yli 99,9 % tarkkuuden lyhyen aikavälin varmentamisessa (katso taulukko 1).

Näppäily- ja hiiridynamiikka vaikuttavat osoittavan eniten potentiaalia käyttäytymisbiometriikan menetelmistä. Shi ym. (2023) osoittavat tutkimuksessaan näppäilydynamiikan varteenotettavuuden lyhyen aikavälin varmentamisprosesseissa, joissa uusien algoritmien avulla pystyttiin tunnistamaan oikea käyttäjä 89.22 % tarkkuudella. Tämä on huomattava parannus aikaisempiin tuloksiin verrattuna, joissa varmentaminen suoritettiin 75,89 % ja 79,48 % tarkkuudella.

Kosketusnäyttöpohjaiset menetelmät ovat myös osoittautuneet tehokkaiksi. Frank, ym. (2013) toteuttamassa ”touchalytics”-tutkimuksessa, jossa hyödynnettiin kosketusnäyttöpohjaista biometriikkaa, saavutettiin lyhyen aikavälin varmentamisessa 13 %:n EER, mikä vastaa 87 % tarkkuutta. Pitkäaikaisessa varmentamisessa, jonka kesto tutkimuksessa oli 11–43 sekuntia, saavutettiin 2–3 %:n EER, mikä vastaa 98–97 % tarkkuutta. Nämä tulokset osoittavat, että kosketusnäyttöpohjainen biometriikka voi tarjota korkean tason turvallisuutta ja käyttäjäkohtaista räätälöintiä, mikä tekee siitä arvokkaan työkalun mobiililaitteiden turvallisuuden parantamiseen. Agrawalin ja Sharman (2022) tutkielmassa koottiin useita kosketusnäyttödynamiikkaa tarkastelleita tutkimuksia, joissa saavutettiin samantapaisia tuloksia kuin Frank ym. (2013) tutkimuksessa. Agrawal ja Sharman painottavat piirteiden yhdistelyä ja niitä analysoimalla voidaan parantaa autentikointijärjestelmän tarkkuutta ja turvallisuutta. Kosketusdynamiikan havaittiin myös toimivan loistavasti esimerkiksi kaksivaiheisen tunnistautumisen menetelmänä osana salasana pohjaisia tunnistautumisen menetelmiä.

Aikaisemmin mainittu puheen- ja äänentunnistuksen käyttö tietoturvallisuudessa puolestaan kohtaa haasteita. Meng ym. (2020) tutkimuksessaan saavuttivat pitkän aikavälin varmentamisessa 95–96 % tarkkuuden, mikä on korkeampi kuin aikaisemmin käytetyillä menetelmillä, mutta testaus vaati suuremman aikaikkunan ja dataa tuli kerätä kolmen minuutin ajanjaksolta. Vaikka nämä haasteet asettavat rajoituksia menetelmän käytännöllisyydelle, puheen- ja äänentunnistusmenetelmät osoittavat silti merkittävää potentiaalia tunnistautumismenetelmänä teknologian kehittyessä.

El-Sayed ym. (2022) tutkimuksessa käytetty algoritmi, joka hyödynsi eri käyttäytymisbiometriikan menetelmien kombinaatioita, saavutti 99 % tarkkuuden käyttäjien varmentamisessa. Tutkimuksessa yhdistettiin näppäily- ja kosketusdynamiikan metodeja ihmisen liikehdinnän mittaamiseen, jota seurattiin älylaitteen sisäisillä sensoreilla. Nämä sensorit tallensivat puhelimen liikuttamista kolmessa ulottuvuudessa sekä puhelimen kääntämisen ranteen liikkeillä. Tutkimus osoittaa, että erityisesti käyttäytymisbiometriikan menetelmien yhdistelyllä potentiaalia toimia jopa yksittäisenä varmentamisen menetelmänä.



KUVIO 7 Puhelimen liikkeen datan kerääminen. (Mukaillen El Sayed ym. 2022)

TAULUKKO 1 Biometrisen tunnistautumisen menetelmiä

Tutkijat	Menetelmä	Vuosi	Tarkkuus
Bhattacharyya ym.	Iiris (Fyysinen biometriikka)	2009	99,99 %
Yang ym.	Sormenjälki (fyysinen biometriikka)	2019 (Tutkielman tutkimukset 2011–2017)	Kootusti ~99,9 %
Albakri & Alghowinem	Kasvot 3D (fyysinen biometriikka)	2018	97–100 %
Jenkins ym.	Kasvot 2D (fyysinen biometriikka)	2014	97,5–98,1 %
Kim ym.	Sydänsähkökäyrä (ECG) (fyysinen biometriikka)	2019	95 %
Frank ym.	Kosketusnäyttödynamiikka	2012	97–98 %
Agrawal & Sharma	Kosketusnäyttödynamiikka	2022 (Tutkielman	Kootusti ~95 %

		tutkimukset 2012–2016)	
Zhao ym.	Kosketusnäyttödynamiikka	2013	92,19–97,48 %
El-Sayed ym.	Yhdistelmä näppäily- ja kosketusnäyttödynamiikkaa sekä liikehdintää.	2022	99 %
Clarke & Furnell	Näppäilydynamiikka	2007	87,8 %
Tewari & Verma	Näppäilydynamiikka	2022	98,57 %
Meng ym.	Puheen- ja äänentunnistus	2020	95–96 %
Shi ym.	Näppäily- ja hiiridynamiikka	2023	89,22 %
Shen ym.	Hiiridynamiikka	2010	97–99 %
Zheng ym.	Hiiridynamiikka	2011	98,1–98,7 %

Vaikka käyttäytymisbiometriikka tarjoaa merkittäviä parannuksia ja mahdollisuuksia tietoturvaan, se ei nykytilassaan välttämättä korvaa fyysistä biometriikkaa. Fyysinen biometriikka, kuten sormenjäljet ja kasvojentunnistus, tarjoaa edelleen korkeimman tason tarkkuuden ja luotettavuuden. Lisäksi fyysinen biometriikka vaatii käyttäytymisbiometriikkaan verrattuna huomattavasti vähemmän dataa (katso kuvio 2), mikä tekee datan keräämisestä ja säilömisestä suoraviivaisempaa ja vähemmän riskialtista. Useissa tutkimuksissa myös painotettiin datan keräämisestä syntyvää taakkaa käyttäjälle. Fyysisen biometriikan kertaluontoinen data sopii paremmin käyttäjäystävällisempään lyhyen aikavälin tunnistautumiseen. Käyttäytymisbiometriikkaa voidaan kuitenkin hyödyntää tehokkaana tukitoimintona ja toissijaisena tietoturvallisuuden työkaluna. Esimerkiksi käyttäytymisbiometriikan menetelmiä voidaan käyttää monivaiheisissa autentikointiprosesseissa, joissa ne toimivat lisäturvana fyysisen biometriikan rinnalla. Tämä lisää kokonaisvaltaisen tietoturvajärjestelmän monipuolisuutta ja vahvistaa sen kykyä suojata käyttäjien tietoja tehokkaasti eri tilanteissa.

Jain ym. (2016) tukevat tätä näkemystä ja painottavat katsauksessaan sekä käyttäytymisbiometriikan että fyysisen biometriikan merkitystä tietopohjaisten tunnistautumismenetelmien rinnalla. He kannustavat laajentamaan käsitystä biometriikasta ja tutkimaan erityisesti käyttäytymisbiometriikan tarjoamia mahdollisuuksia, jotka voivat täydentää perinteisiä menetelmiä uusin, innovatiivisin tavoin. Tämä integraatio mahdollistaa monipuolisemmat ja joustavammat turvallisuusratkaisut, jotka ovat yhä tärkeämpiä digitaalisen toiminnan laajetessa.

On myös huomioitavaa, että tässä tutkielmassa käsitellyt tutkimukset eivät tutki kaupallisia käyttäytymisbiometriikan ratkaisuja. Useissa tutkimuksissa hyödynnetään kokeellisia ja uusia menetelmiä, joita ei välttämättä vielä ole optimoitu.

3.3 Käyttäytymisbiometriikan haasteet

Käyttäytymisbiometriikan isoimpana haasteena on etiikka, erityisesti liittyen datan keräämiseen ja säilyttämiseen. Se herättää merkittäviä kysymyksiä, erityisesti kun otetaan huomioon teknologian perustuminen henkilökohtaisiin käyttäytymistietoihin, jotka sisältävät herkkää käyttäjäkohtaista ja erittäin yksilöllistä tietoa. Menetelmät, kuten näppäilydynamiikka, selauskäyttäytyminen, puheentunnistus, kosketusnäyttödynamiikka ja hiiridynamiikka, vaativat suurten datamäärien keräämistä ja analysointia (Alzubaidi & Kalita, 2016). Tällainen data voi sisältää yksityiskohtaisia tietoja henkilön fyysisistä ja psykologisista ominaisuuksista, mikä asettaa korkeat vaatimukset datan käsittelyn turvallisuudelle ja eettisyydelle. Fyysisen biometriikan menetelmät perustuvat pienempien datamäärien prosessointiin, mikä lieventää huomattavasti edellä mainittuja ongelmia. Lien ym. (2023) nostavat tutkielmassaan esille samoja aiheita ja painottavat esimerkiksi biometrisen tunnistautumisen datasuojaamisen tutkimuksen puutetta.

Käyttäytymisbiometriikan yksi keskeinen eettinen kysymys on datan keräämisen luvallisuus. On tärkeää, että käyttäjiltä saadaan selkeä suostumus ennen heidän käyttäytymistietojensa keräämistä. Tämä suostumus tulisi olla perusteltu, tietoinen ja vapaaehtoinen. Käyttäjän tulisi ymmärtää, mitä tietoja kerätään, mihin tarkoitukseen ja miten tietoja säilytetään ja käsitellään. Lisäksi datan keräämisen läpinäkyvyys ja avoimuus ovat olennaisia, jotta voidaan varmistaa käyttäjän luottamus ja suostumuksen pätevyys.

Erityisesti käyttäytymisbiometriikassa dataa kerätään aktiivisesti käyttäjistä, sekä heidän ympäristöistään, mikä mahdollistaa herkän tiedon vuotamisen tai väärinkäytön (Lien ym. 2023). Näiden henkilötietojen väärinkäyttö voi johtaa vakaviin yksityisyyden loukkauksiin. On mahdollista, että kerättyä dataa voidaan käyttää käyttäjien profilointiin ja seurantaan ilman heidän tietämystään tai suostumustaan. Esimerkiksi puheentunnistustietoja voitaisiin teoriassa käyttää henkilökohtaisten keskustelujen salakuunteluun tai manipulointiin. Samoin, hiiri- ja kosketusnäyttödynamiikka voivat paljastaa paljon käyttäjän tavoista käyttää älylaitteita ja mahdollisista fyysisistä rajoitteista. Näillä tiedoilla pystytään myös mahdollisesti tunnistamaan käyttäjä tilanteissa, joissa hän toimii anonyymisti. On myös mahdollista, että biometrisen datan analysointi voi johtaa virheellisiin tuloksiin, jos dataa ei käsitellä asianmukaisesti tai jos se sisältää virheitä. Näiden riskien hallinta edellyttää vahvoja lainsäädännöllisiä ja teknologisia kehyksiä, jotka takaavat datan turvallisen käsittelyn ja suojaavat yksilöiden yksityisyyttä. Lainsäädännön tulisi määritellä selkeät säännöt siitä, kuka voi kerätä biometristä dataa, miten sitä saa käyttää ja miten pitkään sitä saa säilyttää. Teknologiset ratkaisut, kuten datan anonymisointi ja pseudonymisointi, voivat myös auttaa minimoimaan yksityisyyden riskejä. On tärkeää, että kehitetään ja noudatetaan eettisiä ohjeistuksia ja säännöksiä, jotka suojelevat yksilöitä samalla kun hyödynnetään käyttäytymisbiometriikan tarjoamia mahdollisuuksia. Tämän

saavuttamiseksi on välttämätöntä ylläpitää jatkuvaa dialogia teknologian kehittäjien, käyttäjien ja sääntelyviranomaisten välillä, jotta voidaan varmistaa, että käyttäytymisbiometriikkaa käytetään vastuullisesti ja oikeudenmukaisesti.

3.4 Käyttäytymisbiometriikan hyödyt ja tulevaisuus

Käyttäytymisbiometriikan tulevaisuutta määrittää useat eri tekijät, kuten teknologian kehittyminen, yksilöiden tietoturvatarpeet ja yhteiskunnalliset muutokset. Kuten aiemmin mainitussa Jain, ym. (2006) tutkimuksessa kerrottiin, on biometrinen tunnistautuminen kehittynyt merkittäväksi tietoturvan työkaluksi viime vuosikymmeninä ja erityisesti käyttäytymisbiometriikka on kokenut valtavia muutoksia ja kehitystä käytön yleistyessä.

Teknologian kehittymisen myötä käyttäytymisbiometriikan tarkkuus ja luotettavuus tulevat parantumaan. Kuten luvusta 3.2 huomataan, on käyttäytymisbiometriikan tarkkuus edennyt huomattavasti vanhemmista tutkimuksista. Tekoäly ja koneoppiminen ovat keskeisiä tekijöitä tässä kehityksessä (Purgason & Hibler, 2012), sillä ne mahdollistavat entistä tarkempien käyttäjäprofiilien muodostamisen ja monimutkaisempien käyttäytymismallien analysoinnin. Tämän ansiosta käyttäytymisbiometriikka voi tulevaisuudessa toimia itsenäisenä turvallisuusmenetelmänä ilman tarvetta yhdistää sitä muihin tunnistautumistekniikoihin.

Käyttäytymisbiometriikan soveltamisala myös laajenee. Nykyisten menetelmien, kuten näppäilydynamiikan ja kosketusnäyttödynamiikan, soveltaminen on oletettavasti vain ensiaskel käyttäytymisbiometriikan menetelmien soveltamisessa. Uusia menetelmiä kehitetään jatkuvasti, ja jo olemassa oleville menetelmille voidaan löytää uusia käyttökohteita.

Kuitenkin suurimmaksi potentiaaliseksi esteeksi käyttäytymisbiometriikan laajemmalle soveltamiselle tulevaisuudessa voivat nousta tietoturvaan ja yksityisyydensuojaan liittyvät haasteet sekä niihin kytkeytyvät yhteiskunnalliset muutokset. Useat tämän tutkielman tutkimukset ja erityisesti Bhattacharyya ym. (2009) korostavat mahdollisia yksityisyyteen ja identiteetin vaarantamiseen liittyviä riskejä, sillä käyttäytymisbiometriikka edellyttää merkittävästi enemmän dataa ja tiedonkeruuta verrattuna sen fyysisiin vastineisiin. Kun otetaan huomioon nykyinen herkkä tietosuojaympäristö ja ihmisten skeptisyys informaation keräämiselle voi käyttäytymisbiometriikan laaja implementointi aiheuttaa ongelmia.

4 YHTEENVETO

Tässä tutkielmassa käsiteltiin kirjallisuuskatsauksen muodossa käyttäytymisbiometriikan varteenotettavuutta henkilöllisyyden varmentamisessa jatkuvasti muuttuvassa digitaalisessa ympäristössä, jossa jatkuvat muutokset luovat tarpeen uusille tietoturvallisuuden työkaluille. Erityistä huomiota kiinnitettiin menetelmien esittelyyn, käytäntöön ja haasteisiin, joita liittyy käyttäytymisbiometriikan implementointiin.

Tutkielman tavoitteena on esitellä ja tunnistaa käyttäytymisbiometriikan tietoturvallisia käyttötarkoituksia ja käsitellä niiden varteenotettavuutta. Tutkielmassa vertaillaan käyttäytymisbiometriikkaa ja fyysistä biometriikkaa ominaisuuksien ja tehokkuuden kannalta sekä pyritään tunnistamaan uusia käyttökohteita ja arvioimaan niiden nykyistä tehokkuutta.

Tutkielma toteutettiin kirjallisuuskatsauksena. Lähdeaineisto on haettu pääsääntöisesti Web of Science- ja Google Scholar -tietokannoista. Hakutermeinä on käytetty muun muassa biometrics, behavioral biometrics, security, authentication ja dynamics. Lähdeaineistoksi valittiin mahdollisimman tuoreita artikkeleita siten, että lähes kaikki artikkelit on julkaistu vuoden 2010 jälkeen. Poikkeukset koskevat artikkeleita, jotka käsittelevät aiheen historiaa tai sisältävät olennaisia määritelmiä. Tuoreuden lisäksi lähteiksi pyrittiin valitsemaan artikkeleita, joilla oli mahdollisimman paljon viittauksia. Aiheen ajankohtaisuuden vuoksi lähdeaineistoon sisällytettiin myös uusia tutkimuksia, joilla ei vielä ole paljon viittauksia tuoreutensa vuoksi. Tutkielmassa hyödynnettiin lisäksi aihetta sivuavia tutkimuksia vertailun vuoksi.

Tutkielmassa pyrittiin vastaamaan kahteen kysymykseen:

- Miten käyttäytymisbiometriikkaa voidaan hyödyntää tietoturvallisuudessa?
- Kuinka varteenotettava tietoturvallisuuden työkalu käyttäytymisbiometriikka on?

Tutkielma osoittaa, että käyttäytymisbiometriikkaa voidaan hyödyntää tietoturvallisuudessa lähtökohtaisesti tukitoimintona, mutta teknologian kehittyessä myös ensisijaisena toimintona. Lisäksi käyttäytymisbiometriikka osoittaa potentiaalia uudenlaisissa tietoturvatoiminnoissa, kuten taustavalvonnassa, jossa se voi toimia lisäkerroksena perinteisten tietoturvamenetelmien rinnalla. Tämä korostaa käyttäytymisbiometriikan monipuolisuutta ja sen potentiaalia tulevaisuuden tietoturvaratkaisuissa.

Tutkielmassa havaittiin, että käyttäytymisbiometriikka ei ole vielä fyysisen biometriikan tasolla, mutta se on osoittanut huomattavaa parannusta verrattaessa vanhempia ja uudempia tutkimuksia. On myös huomioitava, että tässä tutkielmassa analysoidut tutkimukset eivät käsitelleet kaupallisia käyttäytymisbiometriikan menetelmiä, jotka voivat olla tehokkaampia. Tarkempien ja arvokkaampien tutkimustulosten saavuttamiseksi olisi yleistä tutkimusta jatkettava ja erityisesti tutkittava lisää menetelmiä, jotka hyödyntävät useita käyttäytymisbiometriikan menetelmiä.

Käyttäytymisbiometriikan hyödyntäminen ei ole vailla haasteita. Suurimmat kysymykset liittyvät kerättävän datan määrään ja tietosuojaan. Tietoturvan asiantuntijoiden ja tutkijoiden on kehitettävä strategioita, jotka huomioivat biometrisen datan herkkyyden ja käyttäjien yksityisyyden suojan. Käyttäjäprofiilien vuotaminen ja väärinkäyttö on todellinen riski, ja käyttäytymisbiometriikka vaatii jatkuvaa valppautta ja kriittistä suhtautumista kerättävään sisältöön erityisesti henkilökohtaisten tietojen käsittelyssä. On välttämätöntä kehittää tehokkaita anonymisointimenetelmiä ja varmistaa tietoturvakäytäntöjen tiukka noudattaminen.

Tutkielma korostaa myös tarvetta jatkotutkimuksille käyttäytymisbiometriikan alalla erityisesti koskien jo olemassa olevia menetelmiä. Teknologian kehittyessä on välttämätöntä ymmärtää yksityiskohtaisemmin, miten erilaiset käyttäytymisbiometriikan menetelmät voivat parantaa tietoturvaa vaarantamatta yksilön yksityisyyden suojaa. Eettisten ja lainsäädännöllisten puitteiden kehittäminen on keskeistä, jotta voidaan varmistaa, että käyttäytymisbiometriikkaa hyödynnetään vastuullisesti ja käyttäjien oikeudet turvataan. Tämä sisältää tutkimuksen siitä, miten käyttäytymisbiometriikan keräämiä tietoja säilytetään, käytetään ja suojataan. On myös tärkeää tutkia käyttäytymisbiometriikan vaikutuksia eri väestöryhmiin ja varmistaa, että tekniikat ovat oikeudenmukaisia ja syrjimättömiä. Jatkotutkimukset voivat myös tutkia käyttäytymisbiometriikan potentiaalia uusissa sovelluksissa, kuten reaaliaikaisessa käyttäjäseurannassa ja ennakoivassa analytiikassa, mikä voisi tarjota entistä dynaamisempia ja joustavampia tietoturvaratkaisuja. Tämän vuoksi on tärkeää kehittää monitieteistä tutkimusta, joka yhdistää teknologiset innovaatiot, eettiset näkökohdat ja lainsäädännölliset vaatimukset, jotta käyttäytymisbiometriikka voi saavuttaa täyden potentiaalinsa tietoturvan parantamisessa.

LÄHTEET

Agrawal, R., & Sharma, P. (2022). A study of touch dynamics biometrics authentication. International Journal of Scientific Research in Engineering and Management (IJSREM), 6(7). Haettu 29.05.2022 osoitteesta: https://www.semanticscholar.org/paper/A-Study-of-Touch-Dynamics-Biometrics-Authentication-Agrawal/894a69150e4c9e0a4776643cebae9d82a9cc887d

Albakri, G., & Alghowinem, S. (2019). The effectiveness of depth data in liveness face authentication using 3D sensor cameras. Sensors, 19(8), 1928. Haettu 06.06.2024 osoitteesta: https://doi.org/10.3390/s19081928

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) 352-358. IEEE.

Altwaijry, N. (2023). Authentication by keystroke dynamics: The influence of typing language. Applied Sciences, 13(20), 11478. Haettu 11.02.2024 osoitteesta: https://www.mdpi.com/2076-3417/13/20/11478

Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials, 18*(3), 1998-2026.

Ahmed, A. A. E., & Traore, I. (2007). A new biometric technology based on mouse dynamics. IEEE Transactions on dependable and secure computing, 4(3), 165-179.

Ballard, L., Lopresti, D., & Monrose, F. (2007). Forgery quality and its implications for behavioral biometric security. IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, 37(5), 1107-1118. Haettu 14.03.2024 osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/4305263

Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. Computers & Security, 43, 77-89.

Barbosa, M., Brouard, T., Cauchie, S., & De Sousa, S. M. (2008). Secure biometric authentication with improved accuracy. In Information Security and Privacy: 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008. Proceedings 13 (pp. 21-36). Springer Berlin Heidelberg.

Bhattacharyya, D., Ranjan, R., Alisherov, F. A., & Choi, M. (2009). Biometric authentication: A review. International Journal of u- and e- Service, Science and Technology, 2(3), 13-28.

Biometrics Institute (2024) Physiological and Behavioural Biometrics. Luettu 13.03.2024 osoitteesta: https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/

Clarke, N. L., & Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. International Journal of Information Security, 6(1), 1-14. https://doi.org/10.1007/s10207-006-0006-6

El-Kenawy, E. S. M., Mirjalili, S., Abdelhamid, A. A., Ibrahim, A., Khodadadi, N., & Eid, M. M. (2022). Meta-Heuristic Optimization and Keystroke Dynamics for Authentication of Smartphone Users. Mathematics, 10(2912). Haettu 03.03.2024 osoitteesta: https://doi.org/10.3390/math10162912

Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Transactions on Information Forensics and Security, 8(1), 136-148. Haettu 31.01.2024 osoitteesta: https://ieeexplore.ieee.org/document/6331527

He, D., & Wang, D. (2015). Robust Biometrics-Based Authentication Scheme for Multiserver Environment. IEEE Systems Journal, 9(3), 816-823. Haettu 01.03.2024 osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/6733264

IATE (Interactive Terminology for Europe). (2024). Biometric Data. Haettu 07.03.2024 osoitteesta https://iate.europa.eu/entry/result/2228682/en

IATE (Interactive Terminology for Europe). (2024). Biometric Verification. Haettu 07.03.2024 osoitteesta https://iate.europa.eu/entry/result/3548809/all

IATE (Interactive Terminology for Europe). (2024). Information Security. Haettu 03.04.2024 osoitteesta https://iate.europa.eu/entry/result/1613434/en

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80-105. Haettu 02.02.2024 osoitteesta: https://doi.org/10.1016/j.patrec.2015.12.013

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security, 1(2), 125-143. Haettu 13.03.2024 osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/1634356/

Jenkins, R., McLachlan, J. L., & Renaud, K. (2014). Facelock: Familiarity-based graphical authentication. PeerJ, 2, e444. https://doi.org/10.7717/peerj.444

Kim, S.-K., Yeun, C. Y., & Yoo, P. D. (2019). An enhanced machine learning-based biometric authentication system using RR-interval framed electrocardiograms. *IEEE Access, PP*(99), 1-1. Haettu 06.06.2024 osoitteesta: https://doi.org/10.1109/ACCESS.2019.2954576

Kyberturvallisuuskeskus (2024) Sähköinen tunnistautuminen. Haettu 03.04.2024 osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Lien, C.-W., & Vhaduri, S. (2023). Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey. ACM Computing Surveys, 56(1), Article 14. Haettu 12.03.2024 osoitteesta: https://doi.org/10.1145/3603705

Lundgren, B., & Möller, N. (2017). Defining information security. Science and Engineering Ethics, 25(2), 419-441. https://doi.org/10.1007/s11948-017-9992-1

Meng, Z., Altaf, M. U. B., & Juang, B.-H. (2020). Active voice authentication. Georgia Institute of Technology. Haettu 02.04.2024 osoitteesta: https://www-sciencedirect-com.ezproxy.jyu.fi/science/article/pii/S1051200420300178

MOT-sanakirja (2024) Biometriikka. Haettu 03.04.2024 osoitteesta https://www.sanakirja.fi/finnish-english/biometriikka

Nassif, A. B., Shahin, I., Attili, I., Azzeh, M., & Shaalan, K. (2019). Speech cRecognition Using Deep Neural Networks: A Systematic Review. IEEE Access, vol. 7, pp. 19143-19165, 2019 Haettu 07.02.2024 osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/8632885

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

Odelu, V., Das, A. K., & Goswami, A. (2015). A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on Information Forensics and Security, 10(9) 1953-1966

Pahwa, R., Tanwar, H. & Sharma, S. (2020). Speech Recognition System: A review. International Journal of Future Generation Communication and Networking. Vol. 13, No. 3. 2547-2559. Haettu 29.05.2024 osoitteesta: https://www.semanticscholar.org/paper/Speech-Recognition-%3A-A-Review-Sharma/2aca31b72a01a728ce44aa51d42e85118979c30c

Purgason, B., & Hibler, D. (2012). Security through behavioral biometrics and artificial intelligence. Procedia Computer Science, 12, 398-403.

Shen, C., Guan, X., & Cai, J. (2010). A hypo-optimum feature selection strategy for mouse dynamics in continuous identity authentication and monitoring. In IEEE International Conference on Information Theory and Information Security (pp. 349-353).

Shi, Y., Wang, X., Zheng, K., & Cao, S. (2023). User authentication method based on keystroke dynamics and mouse dynamics using HDA. Multimedia Systems, 29, 653-668. Haettu 23.04.2024 osoitteesta: https://link-springer-com.ezproxy.jyu.fi/article/10.1007/s00530-022-00997-5

Tewari, A., & Verma, P. (2022). An improved user identification based on keystroke-dynamics and transfer learning. *Webology, 19*(1), 5369-5387. Haettu 29.05.2024 osoitteesta: https://www.webology.org/data-cms/articles/20220123045642pmWEB19360.pdf

TypingDNA (2024) Mouse Dynamics. Haettu 20.03.2024 osoitteesta https://www.typingdna.com/glossary/what-is-mouse-dynamics-and-how-it-works

Yang, W. C., Wang, S., Hu, J. K., Zheng, G. L., & Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry 2019, 11(2). Haettu 30.05.2024 osoitteesta: https://www.mdpi.com/2073-8994/11/2/141

von Solms, B. (2001). Corporate governance and information security. Computers & Security, 20(3), 215–218. Haettu 07.06.2024 osoitteesta: https://www.academia.edu/download/29371330/10.1.1.103.1168.pdf

Zhao, X., Feng, T., & Shi, W. (2013). Continuous mobile authentication using a novel graphic touch gesture feature. In 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS) (pp. 1-6). IEEE. https://doi.org/10.1109/BTAS.2013.6712747

Zheng, N., Paloski, A., & Wang, H. (2011, October). An efficient user verification system via mouse movements. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (pp. 139-150).